UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Red and black thumb-drive with the words "Course.com" on one side and a white string attached.

CURRENTLY LOCATED AT SSA OIG OFFICE, GREENSBORO, NC

Case No. 1:19MJ22-1

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A (incorporated herein)

located in the Middle District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B (incorporated herein)

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 641	Theft of Government Funds
18 U.S.C. 1028A	Aggravated Identity Theft
18 U.S.C. 1343	Wire Fraud

The application is based on these facts:
See attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Manuel Pina, Special Agent, SSA OIG
Printed name and title

Sworn to before me and signed in my presence.

Date: 1/22/19 10:05 AM

Judge's signature

City and state: Durham, North Carolina

Joe L. Webster, United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF: RED AND BLACK THUMB-DRIVE WITH THE WORDS "COURSE.COM" ON ONE SIDE AND A WHITE STRING ATTACHED, CURRENTLY LOCATED AT SSA OIG OFFICE, GREENSBORO, NORTH CAROLINA	1:19MJ22-1

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A WARRANT TO SEARCH AND SEIZE ELECTRONIC MEDIA

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of an electronic device, that is, a thumb-drive which is currently in law enforcement possession ("**Subject Device**"). The proposed warrant would authorize the forensic examination of the **Subject Device** for the purpose of identifying electronically stored data more particularly described in **Attachment B**.

2. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth facts that I believe are necessary to establish probable cause to believe that violations of federal criminal offenses, including 18 U.S.C. § 641 (Theft of Government Funds), 18 U.S.C § 1343 (Wire Fraud), and 18 U.S.C § 1028A (Aggravated Identity Theft), have been committed and that evidence of such violations is located within the **Subject Device**. The statements contained in this affidavit are based upon my

investigation, information provided by other law enforcement personnel, and on my experience and training as a Special Agent.

BACKGROUND

3. I am a Special Agent with the U.S. Social Security Administration (SSA), Office of Inspector General (OIG), and have been since June 2011. I have been a Special Agent with other federal agencies since September 2005 and a law enforcement officer since 1999. As part of my duties as a Special Agent with SSA OIG, I investigate the theft and misuse of Social Security funds more fully described below.

4. SSA is an independent agency of the federal government that administers Social Security, a social insurance program consisting of retirement, disability, and survivors' benefits. The SSA also administers the Supplemental Security Income (SSI) program, which is needs-based, for the aged, blind, or disabled.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is a red and black thumb-drive with the words "Course.com" on one side of the thumb-drive and a white string attached for use as a lanyard. Attached to one end of the lanyard is a sticky note containing a handwritten password. The **Subject Device** is currently located in an evidence locker located at the SSA OIG office, 4900 Koger Blvd, Suite 149 Greensboro, North Carolina 27407.

6. The requested search warrant would authorize the forensic examination of the **Subject Device** as described in **Attachment A**, for the purpose of identifying and seizing the electronically stored data within the **Subject Device** for further investigative analysis as described in **Attachment B**.

PROBABLE CAUSE

7. In or around August 2017, SSA OIG in Greensboro, North Carolina received an allegation regarding an SSA employee at the Fayetteville, North Carolina SSA office who was creating Automated One Time Payments (AOTP) on SSI beneficiary accounts and having the payments direct deposited into five different bank accounts that were not associated with the intended beneficiaries. This employee created forty-eight AOTPs, causing approximately $330,000 in SSI funds to be deposited into the five unassociated bank accounts. The use of the beneficiary information occurred without the knowledge and consent of the beneficiaries.

8. Utilizing the electronic SSA system and various bank records, further investigation uncovered four additional bank accounts as well as additional SSI funds that were deposited into those accounts. Between approximately August 2010 and April 2018, over $750,000 in SSI funds were deposited into those nine bank accounts. All accounts were owned or controlled by Stephanie CHAVIS, who was employed as an Operations Supervisor at the Fayetteville SSA office. Further analysis showed the stolen funds from those nine bank accounts were transferred to

CHAVIS's personal bank account. The majority, if not all, of the transactions were conducted on computers.

9. During an interview with SSA OIG on May 8, 2018, CHAVIS admitted to causing the benefits of SSA beneficiaries to be deposited into bank accounts she controlled. At the time, CHAVIS only admitted to owning/controlling the five bank accounts discovered during the initial investigation. When asked about additional accounts, CHAVIS denied the existence of any other bank accounts. CHAVIS admitted to using her supervisory position to influence other SSA employees to create the AOTPs and have them deposited into her bank accounts. CHAVIS denied that anyone else was involved in, or was aware of, her scheme. After the interview, SSA placed CHAVIS on administrative leave.

10. On October 18, 2018, a federal grand jury sitting in the Eastern District of North Carolina returned a thirteen-count indictment against CHAVIS alleging violations of Title 18, United States Code, Sections 641, 1028A, and 1343. After the indictment, SSA changed CHAVIS's employment status from administrative leave to indefinite suspension. Arraignment is currently scheduled for the February 12, 2019 term of court.

11. While cleaning out CHAVIS's work area, the Fayetteville North Carolina SSA office District Manager (DM) discovered the **Subject Device** inside a file cabinet drawer that contained CHAVIS's personal mail. The DM immediately secured the **Subject Device** and mailed it to the SSA OIG office in Greensboro.

12. The **Subject Device** is currently in storage inside the evidence room located at the SSA OIG office in Greensboro. In my training and experience, I know that the device has been maintained in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the **Subject Device** first came into the possession of the SSA OIG Greensboro, North Carolina office.

13. Based on this investigation and my previous knowledge and experience, I know that employees involved in this type of fraud routinely use computers and other electronic equipment, such as thumb-drives, to obtain and store bank account information, accounting ledgers, personal identifying information ("PII"), and other identifiers needed to execute the fraud scheme.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

14. Based on my knowledge, training, and experience, I know that electronic devices, including thumb-drives, can store information for extended periods. This information can sometimes be recovered with forensic tools.

15. The thumb-drive to be examined may contain digital data related to the subject violations in many electronic forms (e.g., electronic records and documents). These constitute both the means of committing and evidence of wire fraud, theft of government property, and aggravated identity theft. The **Subject Device** is, therefore, subject to search and seizure pursuant to Rule 41(e)(2)(B), and may be retained as evidence and as an instrumentality used in the commission of a

crime for a reasonable period of time and must be examined, analyzed, and tested to preserve its evidentiary value.

16. *Probable Cause* – I submit that there is probable cause to believe those records that were once stored on the **Subject Device** may still be stored on it because I know, based on my knowledge, training, and experience, that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools, unless the file is overwritten by a newly saved file. This is so because when a person "deletes" a file, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten.

17. *Forensic Evidence* – As further described in **Attachment B**, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **Subject Device** was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the **Subject Device** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically-stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

18. *Time Required for an Examination* – As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a device has been used, what it has been used for, and who has used it requires considerable time. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Modern storage media can store large volumes of information.

19. *Nature of examination* – Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the **Subject Device** consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire storage media, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

20. *Manner of Execution* – Because this warrant seeks only permission to examine a device already in law enforcement possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I

submit there is reasonable cause for the Court to authorize the execution of the warrant at any time in the day or night.

CONCLUSION

21. Based upon the foregoing and upon my training and experience, I submit that there is probable cause to believe that evidence, fruits, and instrumentalities of violations, or attempted violations, of 18 U.S.C. §§ 641, 1028A, and 1343, may be located within the **Subject Device**. Wherefore, I request that the Court issue a search warrant authorizing examination of the **Subject Device** as described in **Attachment A** to seek the items described in **Attachment B**.

Respectfully submitted,

MANUEL PINA
Special Agent
Social Security Administration
Office of the Inspector General

Subscribed and sworn to before me on January 22, 2019. 10:05 AM

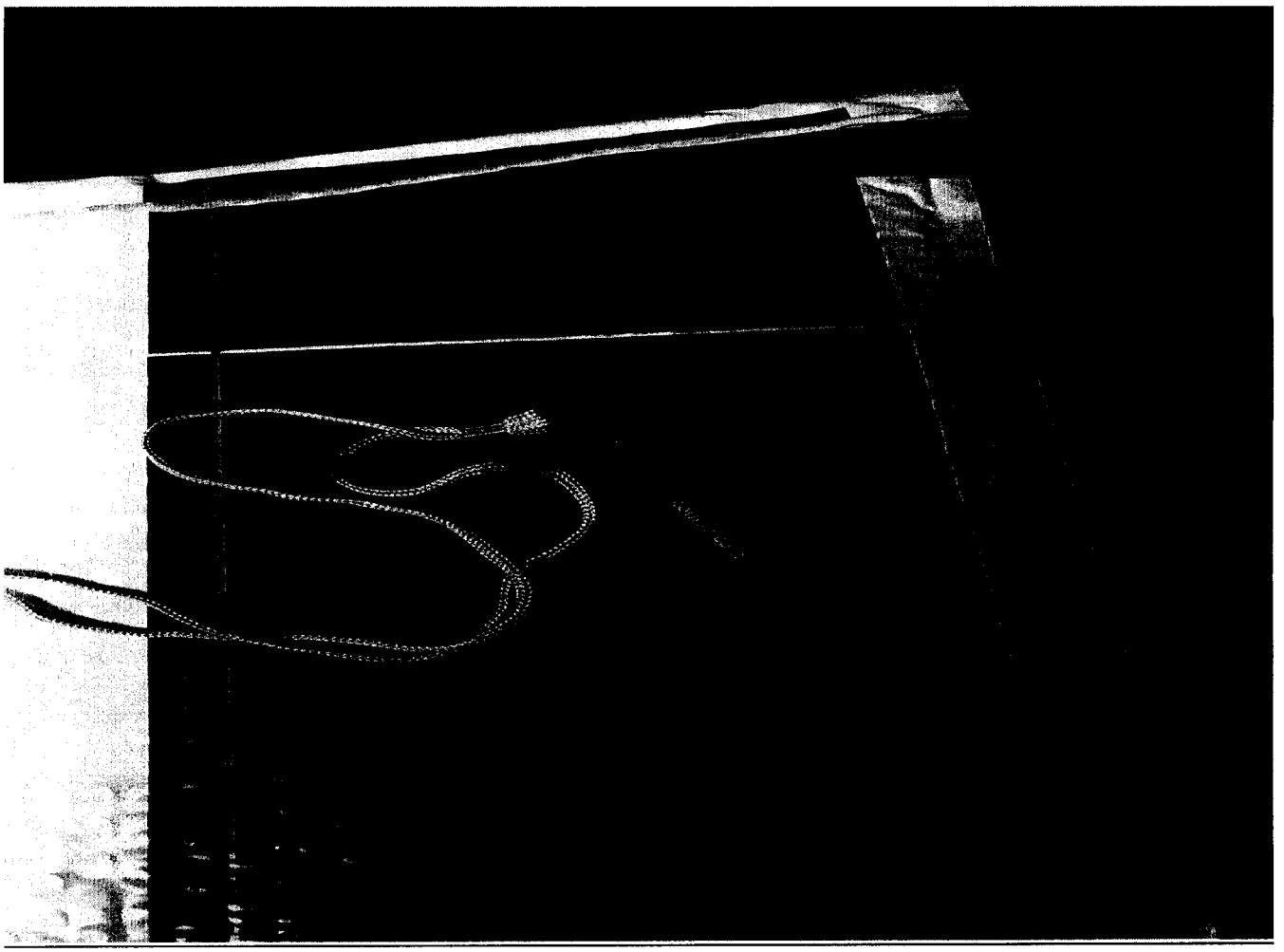
THE HONORABLE JOE L. WEBSTER
UNITED STATES MAGISTRATE JUDGE
MIDDLE DISTRICT OF NORTH CAROLINA

ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant authorizes the forensic examination and evaluation of the following device for the purpose of locating, identifying, and recovering electronically stored information, as described more fully in **Attachment B**, incorporated herein:

One red and black colored thumb-drive with the words "Course.com" on one side of the thumb-drive and a white string attached for use as neck lanyard. The device is currently located in an evidence locker located at the SSA/OIG office at 4900 Koger Blvd, Suite 149 Greensboro, North Carolina 27407.



ATTACHMENT B

PROPERTY TO BE SEARCHED AND/OR SEIZED

This warrant authorizes (i) the search of the property identified in **Attachment A** and (ii) authorizes the seizure of:

(a) evidence of violations of Title 18, United States Code, Sections 641, 1028A, and 1343 ("**Subject Violations**"), which were committed between in or around August 2010 and in or around April 2018, or at earlier times by STEPHANIE CHAVIS;

(b) any item constituting contraband due to the subject violations, fruits of the **Subject Violations**, or other items possessed whose possession is illegal due to the **Subject Violations**; or

(c) any property designed for use, intended for use, or used in committing any **Subject Violations**.

In the form of the following:

1. Records identifying the individual(s) using the device, and any of his/her personal or business contacts or associates (however and wherever written, stored, or maintained), including contact lists, buddy lists, email lists, instant message/direct message names and/or user id's, electronic identification numbers, and passwords;

2. Communication records relating to the Subject Violations, including images/screenshots of SMS (text) messages, images/screenshots of SMS (text) messages, MMS messages, direct messages, photographs, and social media postings;

3. Financial records relating to the Subject Violations, including signature cards, account applications, bank account numbers, account statements, assets, and money transfer transactions;

4. Recordkeeping materials relating to the Subject Violations, including, spreadsheets, logs, notes, text files, books, payment receipts, ledgers, lists and any other transaction records;

5. All photographs, images and/or videos related to the Subject Violations;

6. All data and information that has been deleted by the user of the device and evidence of user attribution showing who used or owned the device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.